

What we claim is:

1. An arrangement for providing wireless data communication services, between a client station and a service providing station or a computer network, each of the client station, service providing station or the computer network being connected to at least one radio transceiver and each being arranged with means to convert data to be transmitted to data packets or data packets to data, *wherein* the radio transceiver is arranged to transmit and/or receive data packets with at least one predetermined, by a user determined or randomly selected low radio frequency, said low radio frequency being within a range of about 1 kHz to about 30 MHz, preferably one or several of: 100-1800 kHz, 1810-1850 kHz, 3500-3800 kHz, 7000-7100 kHz, 10100-10150 kHz, 14000-14350 kHz, 18068-18168 kHz, 21000-21450 kHz, 24890-24990 kHz and 28000-29700 kHz bands.
2. The arrangement according to claim 1, *wherein* said conversion means is a terminal node controller, which automatically divides computer generated messages to be transmitted into data packets with a destination address, keys a transmitting function of the transceiver and sends the data packets through the transceiver.
3. The arrangement according to claim 1, *wherein* the transceiver scans said low radio frequencies for detection of a data packet.
4. The arrangement according to claim 1, *wherein* data is compressed before transmission.
5. The arrangement according to claim 1, *wherein* multiple packets are transmitted on each frequency and/or channels are shared and/or packets are arranged with digital signatures.
6. The arrangement according to claim 1, *wherein* packets are encrypted.
7. The arrangement according to claim 1, *wherein* the client station is arranged with a security key, and an authentication device is arranged to provide an additional layer of security, by verifying whether a client station requesting access to the service provider station posses the security key before access to the service provider is accepted.

8. The arrangement according to claim 1, *wherein* the security arrangement consists of two hardware devices: a security host and a security card, the security host being arranged between the service provider station and the communication means, the security card generates different access codes every time unit, which are synchronized with a code generated at the security host every time unit and at connection time the client sends the code generated by the security card to the host and the code is correct, the security host accepts connection of the client with the service provider server.
9. The arrangement according to claim 1, further including a security host, which prompts the client to enter a username and a password, said security host being arranged to allow the service provider station to initialize the communication means before running the security functions and to directly initialize the communication means connected to the security host without security checks from the security host, before access being accepted.
- 10 15 10. An at least partly wireless data communication network system, including at least one client workstation and at least one service provider station, the wireless data communication being carried out by means of radio signals generated by radio transmitting stations connected to said at least one client workstation and at least one service provider station, in form of data packets, *wherein* the client workstation and the service provider station each are arranged with means to generate a communication protocol (WPPTP) which allows a Point to Point Protocol (PPP) to be tunneled through an IP network over said radio transmitting stations.
- 20 25 11. The system of claim 10, *wherein* said communication protocol (WPPTP) also queries the status of communicating stations, provides in-band management, allocated communication channels and place outgoing calls, notifies the service provider on incoming calls, transmits and receives user data with follow control in both directions, and notifies the service provider about disconnected calls.
- 30 12. The system of claim 10, *wherein* said communication protocol (WPPTP) uses an enhanced Generic Routing Encapsulation (GRE) mechanism to provide a flow and congestion-controlled encapsulated data packets.

13. The system of claim 10, *wherein* said tunnel is defined between pair of Wireless Network access Server (WPNS) and a communication protocol Access Concentrator (WPAC).

14. The system of claim 10, *wherein* the communication protocol (WPPTP) allows functions of devices (32) for providing client stations temporary, on-demand point-to-point wireless network access, to be separated using a client-server architecture.

15. The system of claim 10, *wherein* plurality of connection sessions is multiplexed on a single tunnel.

10

16. The system of claim 10, *wherein* the point-to-point protocol packets are multiplexed and demultiplexed over a single tunnel.

15

17. The system of claim 10, *wherein* the communication protocol Access Concentrator (WPAC) is arranged to interface a network and control radio transceivers or terminal adapters, logically terminate a communications session of a point-to-point-protocol link control protocol, and if needed participate in point-to-point-protocol authentication procedures.

20

18. The system of claim 13, *wherein* the Wireless Network access Server (WPNS) is arranged for channel aggregation and bundle management for point-to-point-protocol multilink protocol, logical termination of various point-to-point-protocol network control protocols and multiprotocol routing and bridging.

25

19. The system of claim 10, *wherein* the radio communication is carried out over low frequency band, preferably in range of about 1 kHz to about 30 MHz.

20. A method for wireless data communication between a client station and a service provider, each being arranged with means to generate data packets and each being connected to a radio transceiver, the method comprising the steps of:

30

- arranging a direct communications path, so-called tunnel, between the client station and the service provider,
- generating a communication protocol (WPPTP) which allows a Point to Point

Protocol (PPP) to be tunneled through an Internet protocol network over said communication path,

- transmitting or receiving said communication protocol by means of said transceivers, and
- transferring said received communication protocol to or from a computer instruction signal.

5

21. The method of claim 20, wherein it further comprises the steps of:

- establishing a Control Connection, controlling the tunnel and sessions assigned to the tunnel,
- maintaining a state for each client station connected,
- creating a session when an end-to-end point-to-point protocol connection is attempted between a client station and a Network access Server (WPNS),
- sending data packets related to a communication session over the tunnel between the communication protocol Access Concentrator (WPAC) and said Network access Server (WPNS).

10

15

20

25

22. The method of claim 20, wherein the control connection is a standard transfer control protocol (TCP) session over which communication protocol (WPPTP) call control and management information are passed.

23. The method of claim 20, wherein for each communication protocol Access Concentrator (WPAC) and Network access Server (WPNS) pair both a tunnel and a control connection exists.

24. The method of claim 20, wherein the control connection is responsible for establishment, management, and release of communication sessions carried through the tunnel.

30

25. The method of claim 20, wherein control connection can be established by either the communication protocol Access Concentrator (WPAC) or the Network access Server (WPNS).

26. The method of claim 24, wherein a sliding window protocol for flow control through the

tunnel is used on the communication protocol by each side of the data exchange.

27. The method of claim 26, wherein the sliding window protocol allows acknowledgment of multiple packets with a single acknowledgment, and all outstanding packets with a sequence number lower or equal to the acknowledgment number are considered acknowledged.
- 5
28. The method of claim 20, wherein time-out calculations are performed using a time that the data packet corresponding to a highest sequence number being acknowledged is transmitted.